UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/607,007	06/29/2000	Thomas P. Hardjono	120-147	7322

34845 7590 11/22/2011

Anderson Gorecki & Manaras LLP
33 NAGOG PARK
ACTON, MA 01720

EXAMINER	
CHOUDHURY, AZIZUL Q	
ART UNIT	PAPER NUMBER
2453	

NOTIFICATION DATE	DELIVERY MODE
11/22/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

handerson@smmalaw.com
officeadmin@smmalaw.com
cmorrissette@smmalaw.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte THOMAS P. HARDJONO and BRADLEY CAIN

Appeal 2009-011754[1]
Application 09/607,007
Technology Center 2400

Before HOWARD B. BLANKENSHIP, JEAN R. HOMERE, and JAMES R. HUGHES, *Administrative Patent Judges*.

HOMERE, *Administrative Patent Judge*.

DECISION ON APPEAL

---

[1] The real party in interest is Nortel Networks, Ltd. (App. Br. 2.)

I. STATEMENT OF THE CASE

Appellants appeal under 35 U.S.C. § 134(a) from the final rejection of claims 1-8, 10-16, 18-25, 27, 28, 31-45, 47-61, 63-68, 70-75, 77-87, 89-105, 108-128, and 131-144.[2] Claims 9, 17, 26, 29, 30, 46, 62, 69, 76, 88, 106, 107, 129, 130, and 145-152 have been canceled. (App. Br. 2.) We have jurisdiction under 35 U.S.C. § 6(b).

We reverse.

Appellants' Invention

According to Appellants, the invention relates to a method and system for allowing a routing device to verify that a key server has authenticated a host device. In particular, after authenticating the host device, the key server provides an access token to the host device to present to the routing device for subsequently verifying the authentication. (App. Br. 1-20.)

Illustrative Claim

Independent claim 1 further illustrates the invention. It reads as follows:

1. A communication system comprising:

a plurality of multicast devices forming a shared multicast distribution tree;

a host device;

a key server; and

---

[2] Both Appellants and the Examiner have mistakenly listed canceled claims as pending in their "Status of Claims", App. Br. at 2, and "Grounds of Rejections", Ans. at 4.

a designated device, separate from the key server, through which the host device requests access to the shared tree associated with a group, wherein:

the host device obtains access information from the key server for the host device to enable the host device to request access to the shared tree associated with the group, the access information including authentication information unique to the host device/group pair, the authentication information including an access token comprising a host identifier, a token identifier and an authentication key for authenticating the host with the designated device;

the designated device obtains the access information associated with the host device/group pair from the key server for enabling the host device to access the shared tree;

the host device sends an access control message to the designated device to join the shared tree; and

the designated device uses the access information to authenticate the host device before adding the host device to the shared tree, including using the token identifier to obtain a group identifier and authentication key from memory in order to verify authentication of the host device.

Prior Art Relied Upon

Watson	U.S. 5,682,478	Oct. 28, 1997
Mittra	U.S. 5,748,736	May 5, 1998
He	U.S. 6,088,451	Jul. 11, 2000 (Filed Jun. 28, 1996)

Rejection on Appeal

Claims 1-8, 10-16, 18-25, 27, 28, 31-45, 47-61, 63-68, 70-75, 77-87, 89-105, 108-128, and 131-144 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Mittra, He, and Watson.

Appellants' Contentions

Appellants argue that the proposed combination of Mittra, He, and Watson would not have taught or fairly suggested a designated device verifying the authentication of a host device by a key server. (App. Br. 19-24; Reply Br. 20-23.) According to Appellants, Mittra discloses a group security controller (GSC) that authenticates host devices, but nowhere discloses a separate device verifying the authentication. (*Id.*)

Examiner's Findings

In response, the Examiner finds that Mittra's disclosure of a key distribution center, and a group server (GSC) teaches or suggests the claimed key server and designated device, respectively. In particular, the Examiner finds that after the GSC authenticates the member nodes, it routes messages to them. (Ans. 19.) Therefore, the pivotal issue before us is as follows:

II. ISSUE

Have Appellants shown that the Examiner erred in finding that Mittra teaches or fairly suggests a designated device that uses authentication key information to verify that a host device has been authenticated by a key server, as recited in independent claim 1?

III. FINDINGS OF FACT

We find that the following enumerated findings of fact (FF) are supported by at least a preponderance of the evidence. *Ethicon, Inc. v. Quigg*, 849 F.2d 1422, 1427 (Fed. Cir. 1988) (explaining the general evidentiary standard for proceedings before the Office).

Mittra

1. Mittra discloses establishing a secure communication via multicast within a group including senders, receivers, a GSC and a trusted intermediary (TI) server. In particular, the GSC and TI server are responsible for maintaining security for the group by authenticating the other multicast members as well as managing group keys to encrypt multicast messages. (Abstr.)
2. Mittra discloses that the TI server and the GSC can be programmed to include router circuitry, and they may have more than one role or function at a time (i.e. sending, receiving, authenticating.) (Col. 6, ll. 49-55.)
3. Mittra also discloses that key distribution centers along with certificate authorities may be used to build a specific implementation of one of the security protocols. (Col. 4, ll. 48-55.)

IV. ANALYSIS

We find error in the Examiner's rejection of independent claim 1, which recites, *inter alia,* a designated device uses authentication key information to verify that a host device has been authenticated by a key

server. In particular, we find that Mittra's disclosure, at best, teaches or suggests that a GSC and an IT server utilize group keys to authenticate members of a multicast group, to authorize them to participate in the multicast session, as well as to route messages to members of said group. (FF. 1-3.) However, we agree with Appellants that while the cited disclosure suggests the GSC and IT server can provide routing functions, it is totally silent on whether such devices are subsequently used to verify that a multicast group member was previously authenticated. Since Appellants have shown at least one error in the Examiner's rejection, we need not address Appellants' other arguments. It therefore follows that Appellants have shown error in the Examiner's rejection of the claims.

Since claims 2-8, 10-16, 18-25, 27, 28, 31-45, 47-61, 63-68, 70-75, 77-87, 89-105, 108-128, and 131-144 also recite the disputed limitations discussed above, Appellants have also shown error in the Examiner's rejection of those claims.

V. DECISION

We reverse the Examiner's rejections of claims 1-8, 10-16, 18-25, 27, 28, 31-45, 47-61, 63-68, 70-75, 77-87, 89-105, 108-128, and 131-144 as set forth above.

REVERSED

Vsh